AAAAA4free & Black Lies

Ólafur Guðmundsson + Marek Vavruša
Filippo Valsorda + ÓG
Black Lies: negative answer with one NSEC record

• Precondition: On-line signing

• Action: generate NSEC, for NXDOMAIN answer, on the fly that matches the QNAME with only RRSIG and NSEC bits set in NSEC record

• Side effect: RCODE == NOERROR

• Result: looks like name exists in cache
“Black Lies” in action
Walking Black lies

- Every name exists \(\implies\) walking is impractical
- Detection: simple walkers are easy to spot
Implementation experience

• All CF signed domains use this
• In use since early last year
• No reports of problems
• Updates RFC4770?
Documenting practice

• Issues?

• Requesting review and publication
  • Standards track ?
  • BCP
  • Informational
AAAA4free == A + AAAA

• Simple idea just add AAAA to queries for A if AAAA exists.

• open questions:
  • what section
  • Q: when ? DO =1 or at least OPT
  • Q: explicit signalling?

• Do we need to prove if AAAA (or A) does not exist
  • If DNSSEC validated ==> save to add
Questions:

- What Section?
- Will resolvers accept this?
  - Drop answer == Bad
  - Ignore == Harmless ==> will improve over time
  - Accept == Great
- Is signaling needed?
  - Only if current resolvers drop answers
Next steps

• Experiment
  • Writing a special purpose server(s) to give out traceable answers
    • unique answer based on QNAME + QTYPE when retrieved from cache
    • Based on APNIC testing framework

• Help us test when ready
• Report on experiments
• Select path forward